



Audit. Evaluate. Comply.

"It really is that simple"

2nd Annual Security Automation Conference and Workshop



Andrew Bove
CTO, Secure Elements, Inc.
Above@Secure-Elements.com





1. Background
2. Our Context -- “Codification”
3. Deriving, Composing and Refining xContent
 - Auditing
 - Vulnerability Scanning
4. Application
5. Results



Secure Elements at a glance ...

- ❑ Secure Elements is dedicated to developing innovative products to evolve the way organizations achieve IT security and compliance
- ❑ We enable organizations to **audit, evaluate, and comply** with internal, industry, and regulatory policies

- ❑ **Venture Capital Funded**
 - ❑ Carlyle Venture Partners
 - ❑ DCM - Doll Capital Management
- ❑ **Founded 2003**
- ❑ **Headquarters in Herndon, Virginia**
 - ❑ Regional US sales offices
 - ❑ Strong industry & channel partners

- ❑ **C5 Security Solutions**
 - ❑ C5 Enterprise Vulnerability Management Suite
 - ❑ C5 Alert Service
 - ❑ C5 Enterprise Security Portal
- ❑ **Markets Served**
 - ❑ Government
 - ❑ Finance, Healthcare, Energy
 - ❑ Critical Infrastructure Providers

Industry Alliances:



ORACLE





C5 Enterprise Vulnerability Management - Features

Audit

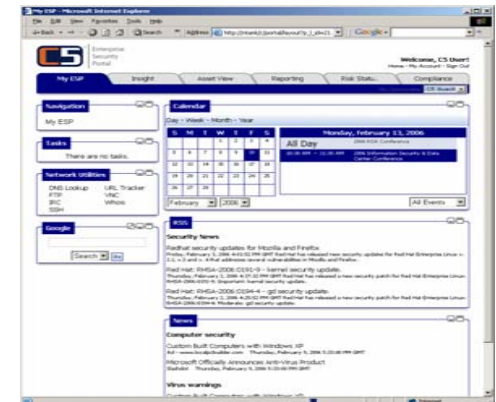
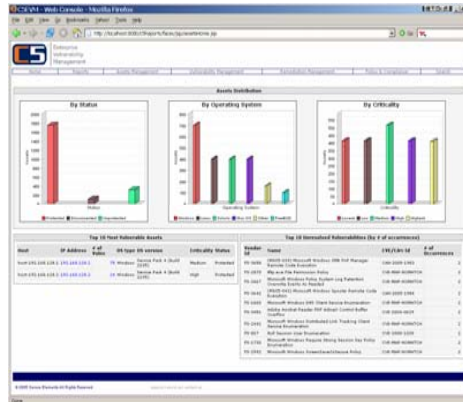
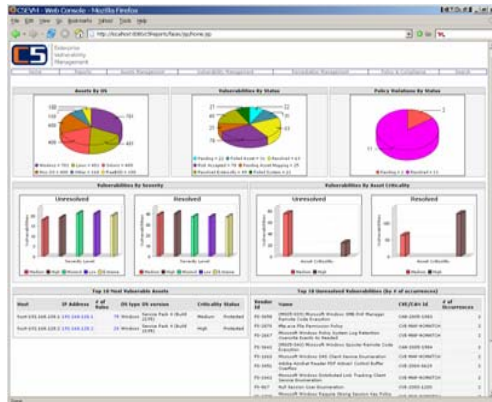
- ☐ Asset inventory on-demand
- ☐ Security vulnerabilities & exposures
- ☐ Compliance score by asset

Evaluate

- ☐ Enterprise security status
- ☐ Compliance score by department
- ☐ Asset criticality vs. risk exposure

Comply

- ☐ Corporate policies
- ☐ Regulated & industry specific
- ☐ Standards & best practices





"The hardest part of building a software system is deciding what to build." - Fred Brooks



- Many Sources of Knowledge
 - Microsoft Windows Security Resource Kit
 - <http://www.securityfocus.com/>
 - <http://sans.org> (SANS Top 20)
 - FISMA
 - SOX
 - CIS
 - HIPPA
- Very Little is Action-able at an Enterprise level



Codification - Checks by Platform

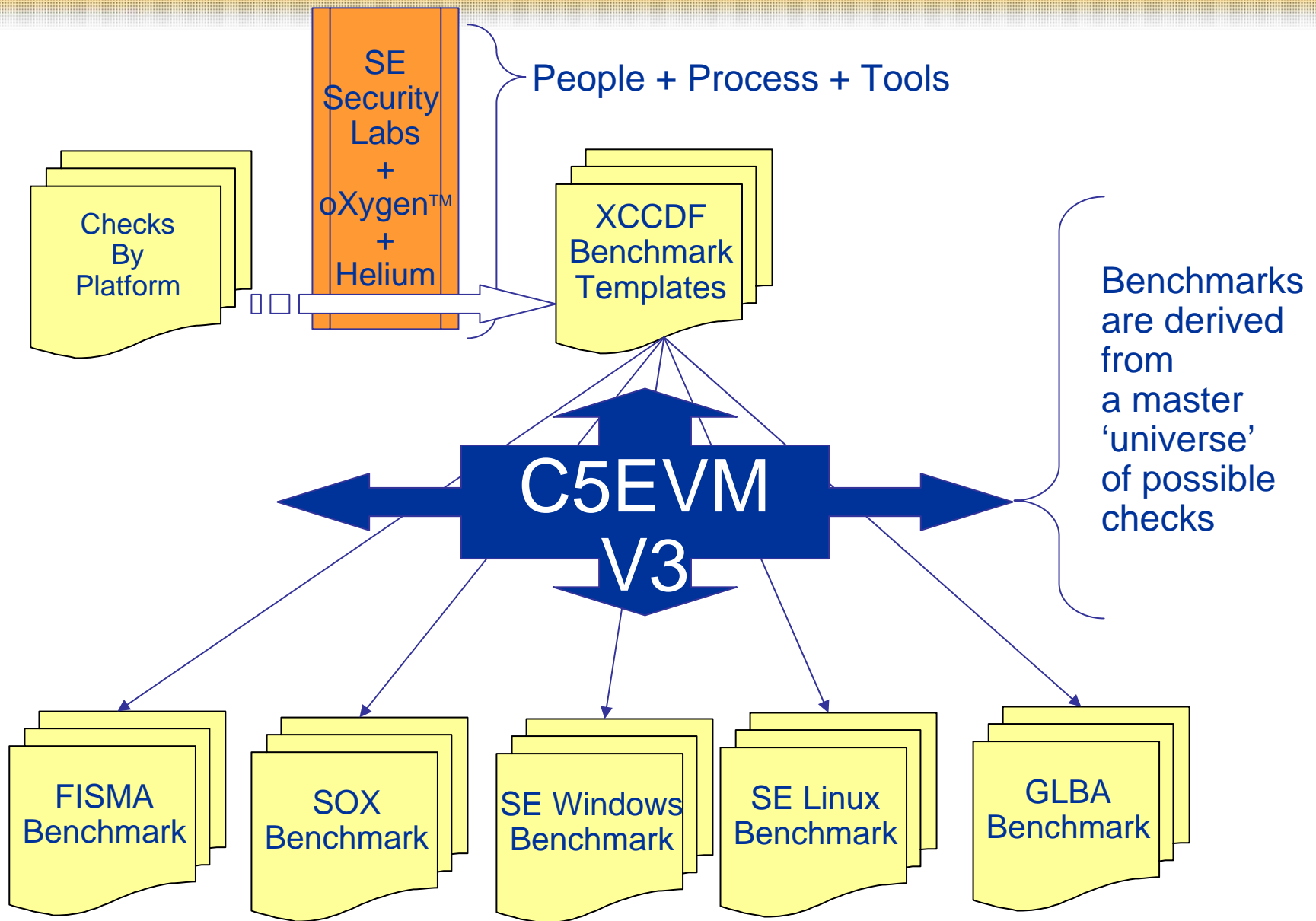
Local Security Policy Settings	WinXP Standalone	WinXP Domain	Win2003 Standalone	Win2003 Domain	WinSrv2000 Standalone	WinSrv2000 Domain	WinPro2000 Standalone	WinPro2000 Domain
Account Policies								
Password Policy								
Enforce password history	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password length	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password must meet complexity requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Store passwords using reversible encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Account Lockout Policy								
Account lockout duration	Yes	Yes	Yes	Yes				Yes
Account lockout threshold	Yes	Yes	Yes	Yes				Yes
Reset account lockout counter after	Yes	Yes	Yes	Yes				Yes
Local Policies								
Audit Policy								
Audit account logon events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes	Yes	Yes		
Audit directory service access	Yes	Yes	Yes	Yes	Yes	Yes		
Audit logon events	Yes	Yes	Yes	Yes	Yes	Yes		
Audit object access	Yes	Yes	Yes	Yes	Yes	Yes		
Audit policy change	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit privilege use	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit process tracking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit system events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Right Assignment								
Access this computer from Network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Act as a part of the operating system	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Add workstations to domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adjust memory quotas for a process	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on locally	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Backup files and directories	Yes	Yes	Yes	Yes			Yes	Yes
Bypass traverse checking	Yes	Yes	Yes	Yes			Yes	Yes
Change the system time	Yes	Yes	Yes	Yes			Yes	Yes
Create a pagefile	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create a token object	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create global objects	SE	SE	SE	SE	SE	SE	SE	SE
Create permanent shared objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Debug programs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny access to this computer from the network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a batch job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on locally	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A

An OVAL Check Exists

SE Produced ~400



Evolution of a XCCDF Benchmark



C5 Command Center

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Home Search Favorites

Address <https://10.2.2.11/CommandCenter/faces/jsp/home.jsp>

Google Search 12 blocked ABC Check AutoLink AutoFill Options



Enterprise
Vulnerability
Manager

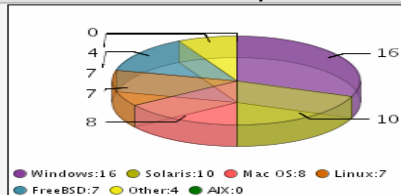
Welcome c5evm_admin

Logout

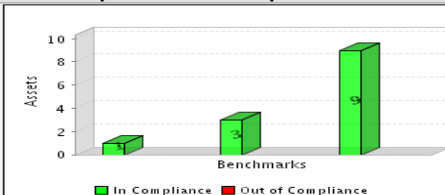
[RSS](#) [Security feed](#)

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

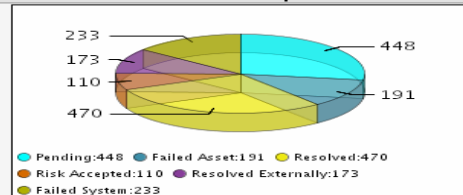
Assets By OS



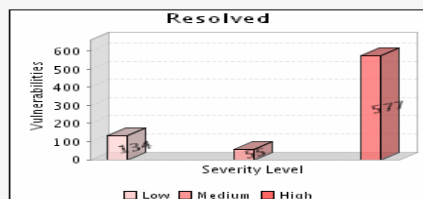
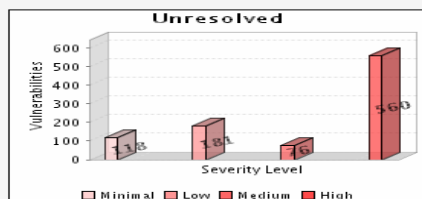
Compliance Results by Benchmarks



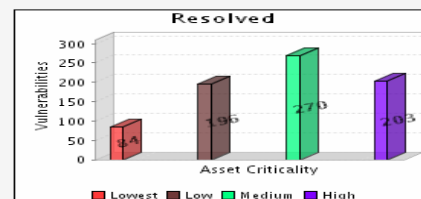
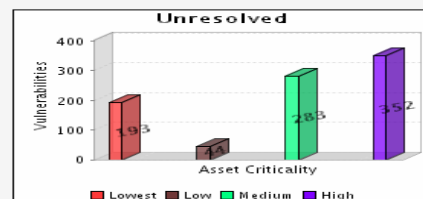
Vulnerabilities By Status



Vulnerabilities By Severity



Vulnerabilities By Asset Criticality



Top 10 Most Vulnerable Assets

[Export to Pdf](#)

Host	IP Address	# of Vulns	OS type	OS version	Criticality	Status
SOJA-ORACLE	10.0.10.171	165	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Protected
W2K3SSP002K31-3	10.2.243.248	138	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Lowest	Protected
W2K3SSP002K31-2	10.2.232.235	132	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Medium	Protected
W2KPRO-SP4-VM2	10.2.251.221	118	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Disconnected
W2KASRV-SP4-VM2	10.2.251.230	77	Microsoft Windows 2000 Advanced Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KSRV-SP4-VM2	10.2.248.237	50	Microsoft Windows 2000 Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KPRO-SP3-VM3	10.2.231.229	49	Microsoft Windows 2000 Professional	Service Pack 3 (Build 2195)	Lowest	Protected
W2KPRO-SP2-VM2	10.2.254.213	46	Microsoft Windows 2000 Professional	Service Pack 2 (Build 2195)	High	Protected
W2KPRO-SP4-VM3	10.2.242.214	30	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	Low	Protected
W2KSRV-SP3-VM2	10.2.241.246	24	Microsoft Windows 2000 Server	Service Pack 3 (Build 2195)	Medium	Protected

Top 10 Unresolved Vulnerabilities (by # of occurrences)

[Export to Pdf](#)

Vendor Id	Name	CVE/CAN Id	Severity	# of Occurrences
oval.org.mitre.oval:def:115	Hyperlink Object Function Vulnerability	CVE-2006-3438	High	10
oval.org.mitre.oval:def:13	Buffer Overrun in HTML Help Vulnerability	CVE-2006-3357	High	8
oval.org.mitre.oval:def:155	User Profile Elevation of Privilege Vulnerability	CVE-2006-3443	High	8
oval.org.mitre.oval:def:21	Microsoft Office Remote Code Execution Using a Malformed GIF Vulnerability	CVE-2006-0007	High	8
oval.org.mitre.oval:def:492	Buffer Overrun in Server Service Vulnerability	CVE-2006-3439	High	8
oval.org.mitre.oval:def:841	Unhandled Exception Vulnerability	CVE-2006-3648	High	8
oval.org.mitre.oval:def:1559	Windows Media Player Plug-in EMBED Vulnerability	CVE-2006-0005	Medium	8
oval.org.mitre.oval:def:723	DNS Client Buffer Overrun Vulnerability	CVE-2006-3441	High	7
oval.org.mitre.oval:def:747	Winsock Hostname Vulnerability	CVE-2006-3440	High	7
oval.org.mitre.oval:def:999	Hyperlink Object Buffer Overflow Vulnerability	CVE-2006-3086	High	7



Deriving Benchmarks Through Adaptation

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS 12 blocked Check AutoLink AutoFill Options

Address https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep1.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Adapt Regulatory Standard

Perform Compliance Audit

Adapt Regulatory Standard - Step 1 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step One - Select benchmark

Step 1 of 4 - Select Benchmark

Benchmark Name : NIST-800-68-53-WinXPPro_XCCDF_09182006

Benchmark Title : SP 800-68: Guidance for Securing Microsoft Windows XP Systems

- ☒ SP 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professionals(NIST-800-68-53-WinXPPro_XCCDF_09182006.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows 2000(se-win2k-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows Server 2003(se-win2k3-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark(se-winxp-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark(services-xccdf.xml)

Forward

All of the content that the system knows about that I am allowed to **adapt** to the enterprise



Adaptation of the NIST Benchmark

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Feeds

Address <https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep2.jsp> Go Links



Welcome c5evm_admin

Logout

RSS security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 2 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Two - Select profiles

Step 2 of 4 - Select Profiles

- ☐ Specialized Security-Limited Functionality-High
- ☐ Enterprise-Low
- ☐ Enterprise-Moderate
- ☒ Enterprise-High
- ☐ Legacy-Low
- ☐ Legacy-Moderate
- ☐ Legacy-High
- ☐ SOHO-Standalone-Low
- ☐ SOHO-Standalone-Moderate
- ☐ SOHO-Standalone-High"

Select the applicable profiles

Back

Forward

Done

Internet

Adaptation of the NIST Rules

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep2.jsp



Welcome c5evm_admin

Logout

[RSS security feed](#)

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 3 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Three - Select rules

Step 3 of 4 - Select Rules

Select All

Select None

Select Rule	Title	Oval Id
<input type="checkbox"/> AuditAccountLoginSuccessOnly	Audit Account Login Success Only	oval:gov.nist.1:def:28
<input checked="" type="checkbox"/> AccountLockoutDuration	Account Lockout Duration	oval:gov.nist.1:def:23
<input checked="" type="checkbox"/> FIPSCryptography	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	oval:gov.nist.1:def:105
<input checked="" type="checkbox"/> MaximumMachineAccountPasswordAge	Domain member: Maximum machine account password age	oval:gov.nist.1:def:65
<input checked="" type="checkbox"/> DomainControllerAuthenticationRequired	Interactive logon: Require Domain Controller authentication to unlock workstation.	oval:gov.nist.1:def:75
<input checked="" type="checkbox"/> LDAPClientSigningRequirements	Network security: LDAP client signing requirements	oval:gov.nist.1:def:98
<input checked="" type="checkbox"/> NTLMSSPBasedClientsSessionSecurity	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	oval:gov.nist.1:def:100
<input checked="" type="checkbox"/> AllowICMPRedirectsDisabled	MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	oval:gov.nist.1:def:113
<input checked="" type="checkbox"/> AuditPolicyChangesSuccessOnly	Audit Policy Changes Success Only	oval:gov.nist.1:def:35
<input checked="" type="checkbox"/> AccountLockoutThreshold-10	Account Lockout Threshold	oval:gov.nist.1:def:24
<input checked="" type="checkbox"/> NTLMSSPBasedClientsSessionSecurity	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	oval:gov.nist.1:def:99
<input checked="" type="checkbox"/> LogonMessageText	Interactive logon: Message text for users attempting to log on	oval:gov.nist.1:def:70
<input checked="" type="checkbox"/> AuditAccessToGlobalObjects	Audit: Audit the access of global system objects	oval:gov.nist.1:def:45
<input type="checkbox"/> AuditObjectAccessDisabled	Auditing of Object Access is Disabled	oval:gov.nist.1:def:38
<input checked="" type="checkbox"/> UnencryptedSMBPasswords	Microsoft network client: Send unencrypted password to third-party SMB servers	oval:gov.nist.1:def:82
<input checked="" type="checkbox"/> RestrictCDROMAccessDisabled	Devices: Restrict CD-ROM access to locally logged-on user only disabled	oval:gov.nist.1:def:58
<input checked="" type="checkbox"/> CredentialsStorage	Network access: Do not allow storage of credentials or .NET Passports for network authentication	oval:gov.nist.1:def:89
<input checked="" type="checkbox"/> ScreenSaverGracePeriod	MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires	oval:gov.nist.1:def:123
<input checked="" type="checkbox"/> SignCommunicationsIfClientAgrees	Microsoft network server: Digitally sign communications (if client agrees)	oval:gov.nist.1:def:85
<input checked="" type="checkbox"/> Disable8Dot3NameCreation	MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames	oval:gov.nist.1:def:119
<input type="checkbox"/> AuditPrivilegeUseDisabled	Audit privilege Use Disabled	oval:gov.nist.1:def:39
<input checked="" type="checkbox"/> DisableAutorunForAllDrives	MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives	oval:gov.nist.1:def:117
<input checked="" type="checkbox"/> ZeroCachedPreviousLogons	Interactive logon: Zero previous logons cached (in case domain controller is not available)	oval:gov.nist.1:def:72
<input checked="" type="checkbox"/> AllowUndockWithoutLoginDisabled	Devices: Allow undock without having to log on disabled	oval:gov.nist.1:def:53
<input checked="" type="checkbox"/> AuditObjectAccessFailureOnly	Audit Object Access Failure Only	oval:gov.nist.1:def:34
<input checked="" type="checkbox"/> SignCommunicationsIfServerAgrees	Microsoft network client: Digitally sign communications (if server agrees)	oval:gov.nist.1:def:81
<input checked="" type="checkbox"/> NameReleaseRequests	MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	oval:gov.nist.1:def:118
<input checked="" type="checkbox"/> RestrictFloppyAccessDisabled	Devices: Restrict floppy access to locally logged-on user only disabled	oval:gov.nist.1:def:59
<input checked="" type="checkbox"/> AnonymousEnumerationOfAccountsAndShares	Network access: Do not allow anonymous enumeration of SAM accounts and shares	oval:gov.nist.1:def:88

[Back](#)

[Forward](#)



Adaptation of the CIS Benchmark

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Feeds

Address <https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep1.jsp> Go Links



Welcome c5evm_admin

Logout

security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 1 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step One - Select benchmark

Step 1 of 4 - Select Benchmark

Benchmark Name :

Benchmark Title :

- ☒ Windows 2000 Professional Operating System Benchmarks(cis-gold-win2000-pro-xccdf.xml)
- ☐ Windows 2000 Server Operating System Benchmarks(cis-gold-win2000-srv-xccdf.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks(cis-win2000-pro-xccdf-1.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks(cis-win2000-pro-xccdf.xml)
- ☐ Windows 2000 Server Operating System Benchmarks(cis-win2000-srv-xccdf.xml)
- ☐ Windows 2000 Operating System Level One Benchmark(cis-win2000-xccdf.xml)
- ☐ Windows XP Professional Benchmark(cis-winxp-xccdf.xml)
- ☐ SP 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professional(NIST-800-68-53-WinXPPro_XCCDF_08242006.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows 2000(se-win2k-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows Server 2003(se-win2k3-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark(se-winxp-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark(services-xccdf.xml)

Forward

Adaptation of the CIS Rules

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Feeds

Address <https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep2.jsp> Go Links



Welcome c5evm_admin

Logout

security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 2 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Two - Select profiles

Step 2 of 4 - Select Profiles

☒ Level II

Back

Forward

© 2005 Secure Elements All Rights Reserved.

[support](#) | [about us](#) | [contact us](#)

Done

Internet

www.secure-elements.com

Adaptation of the CIS Rules

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep2.jsp> Go Links



Welcome c5evm_admin

Logout

[RSS security feed](#)

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 3 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Three - Select rules

Step 3 of 4 - Select Rules

Select All

Select None

Select	Rule Id	Title	Oval Id
<input type="checkbox"/>	audit-dir-srv-access-rul	Audit Directory Service Access: Not Defined	OVAL99002213
<input checked="" type="checkbox"/>	profile-single-rul	Profile single process: Administrators	OVAL99004227
<input checked="" type="checkbox"/>	system-drive-progfiles-rk-rul	%SystemDrive%\Program Files\Resource Kit	OVAL990044118
<input checked="" type="checkbox"/>	max-pw-age-rul	Maximum Password Age: 90 days (as per major requirements)	OVAL99002222
<input checked="" type="checkbox"/>	mess-title-user-logon-rul	Message Title for Users Attempting to Log On: Warning: or custom title.	OVAL990032118
<input checked="" type="checkbox"/>	sys-root-rsh-exe-rul	%SystemRoot%\system32\rsh.exe	OVAL990044136
<input type="checkbox"/>	sec-log-retention-rul	Log Retention	OVAL990022424
<input checked="" type="checkbox"/>	disable-auto-logon-rul	Disable Automatic Logon:	OVAL99003226
<input checked="" type="checkbox"/>	protect-dflt-gateway-rul	Protect the Default Gateway network setting:	OVAL990032215
<input checked="" type="checkbox"/>	mod-firmware-rul	Modify firmware environment values: Administrators	OVAL99004226
<input checked="" type="checkbox"/>	alerter-rul	Alerter Disabled	OVAL9900411
<input type="checkbox"/>	app-log-retention-rul	Log Retention	OVAL990022414

Back

Forward



Adaptation of the C5 STIGS

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.



File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites RSS Feeds

Address <https://10.2.2.3/CommandCenter/faces/jsp/comp/adapt/adaptStep2.jsp>

Go Links

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

[RSS security feed](#)

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 2 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Two - Select profiles

Step 2 of 4 - Select Profiles

- ☒ C5 DISA STIGS - Windows Server 2003
- ☐ C5 Specialized Security - Limited Functionality (SSLF) for Member Servers

[Back](#)

[Forward](#)

© 2005 Secure Elements All Rights Reserved.

[support](#) | [about us](#) | [contact us](#)

Shortcut to adaptStep2.jsp# (secure Web site)

[Internet](#)

www.secure-elements.com



Adaptation of Tolerance of Rules

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Home

Address https://10.2.2.3/CommandCenter/faces/jsp/comp/adapt/adaptStep3.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Step 4 of 4 - Specify value bindings

Please specify value bindings for C5 DISA STIGS - Windows Server 2003 profile

Minimum Password Length

☐ 12 (

The Military Measurement Rule: Measure it with a micrometer, mark it with a piece of chalk, and cut it with an ax.

Alerte

☐ 3 (s

(disabled)

Application Layer External Service

☐ 3 (service_demand_start) ☐ 0 (service_boot_start) ☐ 2 (service_auto_start) ☐ 1 (service_system_start) ☒ 4 (service_disabled)

Application Management Service

☐ 3 (service_demand_start) ☐ 0 (service_boot_start) ☐ 2 (service_auto_start) ☐ 1 (service_system_start) ☒ 4 (service_disabled)

ASP.NET State Service

☐ 3 (service_demand_start) ☐ 0 (service_boot_start) ☐ 2 (service_auto_start) ☐ 1 (service_system_start) ☒ 4 (service_disabled)

COM+ System Application

☐ 3 (service_demand_start) ☐ 0 (service_boot_start) ☐ 2 (service_auto_start) ☐ 1 (service_system_start) ☒ 4 (service_disabled)

Computer Browser

☐ 3 (service_demand_start) ☐ 0 (service_boot_start) ☒ 2 (service_auto_start) ☐ 1 (service_system_start) ☐ 4 (service_disabled)

Distributed Transaction Coordinator

☐ 3 (service_demand_start) ☐ 0 (service_boot_start) ☐ 2 (service_auto_start) ☐ 1 (service_system_start) ☒ 4 (service_disabled)

Back

Save



Adaptation of the Secure Elements Benchmark

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep1.jsp> Go Links



Welcome c5evm_admin

Logout

security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 1 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step One - Select benchmark

Step 1 of 4 - Select Benchmark

Benchmark Name :

Benchmark Title :

- ☐ Windows 2000 Professional Operating System Benchmarks(cis-gold-win2000-pro-xccdf-09182006.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks(cis-gold-win2000-pro-xccdf.xml)
- ☐ Windows 2000 Server Operating System Benchmarks(cis-gold-win2000-srv-xccdf.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks(cis-win2000-pro-xccdf-1.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks(cis-win2000-pro-xccdf.xml)
- ☐ Windows 2000 Server Operating System Benchmarks(cis-win2000-srv-xccdf.xml)
- ☐ SP 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professionals(NIST-800-68-53-WinXPPro_XCCDF_091842006.xml)
- ☒ Secure Elements Best Practices Benchmark - Windows 2000(se-win2k-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows Server 2003(se-win2k3-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark(se-winxp-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark(services-xccdf.xml)

Forward



Adaptation of the Secure Elements Profiles

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.



File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites Print Mail News RSS Feeds

Address <https://10.2.2.11/CommandCenter/faces/jsp/comp/adapt/adaptStep2.jsp> Go Links



Welcome c5evm_admin

Logout

security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 2 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Two - Select profiles

Step 2 of 4 - Select Profiles

☒ Secure Elements Best Practices Profile - Windows 2000

Back

Forward

© 2005 Secure Elements All Rights Reserved.

[support](#) | [about us](#) | [contact us](#)

Done

Internet

www.secure-elements.com



Adaptation of the Secure Elements Rules

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Home

Address https://10.0.10.179/CommandCenter/faces/jsp/adaptStep3.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Adapt Regulatory Standard - Step 3 of 4

Benchmark

Profiles

Rules

Values

Save

Adapt Benchmark - Step Three - Select rules

Title

Rules

Local Security Policy Settings

Account Policies

Password Policy

Enforce Password

Maximum Password

Minimum Password

Minimum Password

Password Complexity

Store Passwords

Account Lockout

Local Policies

Audit Policy

User Right Assignment

Security Options

Event Log Policy

Restricted Groups Policy

System Services Policy

Registry Settings Policy

Hardening TCP/IP Stack

Additional Registry Settings

Permissions

Registry Permissions

File Permissions

Other Hardening Settings

Local Security Policy Settings	WinXP Standalone	WinXP Domain	Win2003 Standalone	Win2003 Domain	WinSrv2000 Standalone	WinSrv2000 Domain	WinPro2000 Standalone	WinPro2000 Domain
Account Policies								
Password Policy								
Enforce password history	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Maximum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password age	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Minimum password length	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password must meet complexity requirements	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Store passwords using reversible encryption	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Account Lockout Policy								
Account lockout duration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Account lockout threshold	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reset account lockout counter after	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Local Policies								
Audit Policy								
Audit account logon events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit account management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit directory service access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit logon events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit object access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit policy change	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit privilege use	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit process tracking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Audit system events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Right Assignment								
Access this computer from Network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Act as a part of the operating system	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Add workstations to domain	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Adjust memory quotas for a process	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on locally	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Allow log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A
Backup files and directories	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Bypass traverse checking	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Change the system time	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create a pagefile	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create a token object	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Create global objects	SE	SE	SE	SE	SE	SE	SE	SE
Create permanent shared objects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Debug programs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny access to this computer from the network	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a batch job	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on as a service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on locally	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Deny log on through Terminal Services	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A

Back

Forward



- XCCDF Allows grouping of OVAL Compliance Tests
- Why Not Group OVAL Vulnerability Tests into a Vulnerability “Job” using XCCDF?

Vulnerability Scanning

C5EVM - Vulnerability Management - Create Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS 12 blocked Check AutoLink AutoFill Options

Address <http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/cscan/createScanStep1.jsp> Go Links

Google Search

C5 Enterprise Vulnerability Management

Welcome c5evm_admin Logout **RSS** security feed

Home Compliance **Reports** Assets Management Vulnerability Management Remediation Management

View Scan Definitions **Create Scan** Perform Scan View Scan Results

Vulnerabilities Home

Create Vulnerability Scan - Step 1 of 3

Benchmark Platforms Rules Save

Create Vulnerability Scan - Step One - Select Benchmark

Step 1 of 3 - Select Scan

Scan Title:

Forward

Internet



Vulnerability Scanning - Platforms

C5EVM - Vulnerability Management - Create Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/cscan/createScanStep2.jsp> Go Links

Google Search 12 blocked Check AutoLink AutoFill Options

C5 Enterprise Vulnerability Management

Welcome c5evm_admin Logout **RSS** security feed

Home	Compliance	Reports	Assets Management	Vulnerability Management	Remediation Management
------	------------	---------	-------------------	--------------------------	------------------------

View Scan Definitions	Create Scan	Perform Scan	View Scan Results
-----------------------	-------------	--------------	-------------------

Vulnerabilities Home

Create Vulnerability Scan - Step 2 of 3

Benchmark **Platforms** Rules Save

Create Vulnerability Scan - Step Two - Select Platforms

Step 2 of 3 - Select Platforms

- ☒ Microsoft Windows 2000
- ☐ Microsoft Windows 95
- ☐ Microsoft Windows 98
- ☐ Microsoft Windows ME
- ☐ Microsoft Windows NT
- ☒ Microsoft Windows Server 2003
- ☒ Microsoft Windows XP

Done Internet



Vulnerability Scanning – Rule Selection

C5EVM - Vulnerability Management - Create Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS 12 blocked Check AutoLink AutoFill Options

Address <http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/cscan/createScanStep2.jsp> Go Links

Google Search

C5 Enterprise Vulnerability Management

Welcome c5evm_admin Logout **RSS** security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

View Scan Definitions Create Scan Perform Scan View Scan Results

Vulnerabilities Home

Create Vulnerability Scan - Step 3 of 3

Benchmark Platforms **Rules** Save

Create Vulnerability Scan - Step Three - Select Rules

Step 3 of 3 - Select Rules

Select All Select None

Select	Rule Id	Title	Oval Id
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:4264	ISA Server Reverse DNS Lookup Results Spoofing	oval:org.mitre.oval:def:4264
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:381	Server 2003 HTML Help Remote Code Execution Vulnerability	oval:org.mitre.oval:def:381
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:1416	FTP Download Destination Tampering Vulnerability (Windows XP)	oval:org.mitre.oval:def:1416
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:231	SQL Server Extended Stored Procedure Parameter Parsing	oval:org.mitre.oval:def:231
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:303	SQL Server LPC Port Buffer Overflow	oval:org.mitre.oval:def:303
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:1591	IE6 RTA Execution Vulnerability (Windows XP)	oval:org.mitre.oval:def:1591

Done Internet

What are these things anyway?

Rule Interrogation

C5EVM - Vulnerability Management - View Scan Definitions - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <https://10.0.10.10/c5Reports/faces/jsp/vulns/vscandef/scanDetail.jsp> Go Links

Google Search 12 blocked Check AutoLink AutoFill Options

C5 Enterprise Vulnerability Management

Welcome Logout **RSS** security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

View Scan Definitions Create Scan Perform Scan View Scan Results

Back

Scan-server2003-T1-ALL Details

Rule Details : oval:org.mitre.oval:def:723
Namespace : http://oval.mitre.org/XMLSchema/oval-definitions-5
Source : windows.tg-oval.xml
Test Id
Reference
Affected Family
Affected Platforms

Affected Products
Pseudo Code

Raw XML : <?xml version="1.0" encoding="UTF-8"?>
<oval:definition id="oval:org.mitre.oval:def:723" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-definitions-5">
 <oval:metadata>
 <oval:title>DNS Client Buffer Overrun Vulnerability</oval:title>
 <oval:affected family="windows">
 <oval:platform>Microsoft Windows 2000</oval:platform>
 <oval:platform>Microsoft Windows XP</oval:platform>
 <oval:platform>Microsoft Windows Server 2003</oval:platform>
 <oval:product>Operating System</oval:product>
 </oval:affected>
 <oval:reference ref_id="CVE-2006-3441"
 ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3441" source="CVE"/>
 <oval:description>Buffer overflow in the DNS Client service in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1</oval:description>
 </oval:metadata>
 <oval:criteria negate="false" operator="OR">
 <oval:criteria comment="Win2K, SP4" negate="false" operator="AND">
 <oval:criterion
 comment="the version of dnsapi.dll is less than 5.0.2195.7100"
 negate="false" test_ref="oval:org.mitre.oval:tst:130"/>
 <oval:extend_definition
 comment="Windows 2000, SP4 is installed"
 definition_ref="oval:org.mitre.oval:def:229" negate="false"/>
 </oval:criteria>
 <oval:criteria comment="WinXP, SP1" negate="false" operator="AND">
 <oval:criterion
 comment="the version of dnsapi.dll is less than 5.1.2600.1863"
 negate="false" test_ref="oval:org.mitre.oval:tst:81"/>
 <oval:extend_definition
 comment="Windows XP, SP1 is installed"
 definition_ref="oval:org.mitre.oval:def:1" negate="false"/>
 </oval:criteria>
 <oval:criteria comment="WinXP, SP2" negate="false" operator="AND">
 <oval:criterion
 comment="the version of dnsapi.dll is less than 5.1.2600.2938"
 negate="false" test_ref="oval:org.mitre.oval:tst:198"/>
 <oval:extend_definition
 comment="Windows XP, SP2 is installed"



Vulnerability Scanning – Rule Selection

C5EVM - Vulnerability Management - Create Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS 12 blocked Check AutoLink AutoFill Options

Address <http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/cscan/createScanStep2.jsp> Go Links

Google Search

C5 Enterprise Vulnerability Management

Welcome c5evm_admin Logout **RSS** security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

View Scan Definitions Create Scan Perform Scan View Scan Results

Vulnerabilities Home

Create Vulnerability Scan - Step 3 of 3

Benchmark Platforms Rules Save

Create Vulnerability Scan - Step Three - Select Rules

Step 3 of 3 - Select Rules

Select All Select None

Select	Rule Id	Title	Oval Id
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:4264	ISA Server Reverse DNS Lookup Results Spoofing	oval:org.mitre.oval:def:4264
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:381	Server 2003 HTML Help Remote Code Execution Vulnerability	oval:org.mitre.oval:def:381
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:1416	FTP Download Destination Tampering Vulnerability (Windows XP)	oval:org.mitre.oval:def:1416
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:231	SQL Server Extended Stored Procedure Parameter Parsing	oval:org.mitre.oval:def:231
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:303	SQL Server LPC Port Buffer Overflow	oval:org.mitre.oval:def:303
<input checked="" type="checkbox"/>	oval:org.mitre.oval:def:1591	IE6 RTA Execution Vulnerability (Windows XP)	oval:org.mitre.oval:def:1591

Done Internet

- Adapted Compliance Content
 - ✓ Various Sources
- Created A Vulnerability Scan

OVAl Scanning

C5EVM - Vulnerability Management - Perform Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS 12 blocked Check AutoLink AutoFill Options

Address http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/pscan/performScanStep1.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

View Scan Definitions

Create Scan

Perform Scan

View Scan Results

Vulnerabilities Home

Perform Vulnerability Scan - Step 1 of 3

Benchmark

Platforms

Assets

Perform

Perform Vulnerability Scan - Step One - Select Benchmark

Step 1 of 3 - Select Scan

MyFirstVulnScan(vulnerability-scan-1156201858873.xml)

Forward



Apply an OVAL Vulnerability Scan

C5EVM - Vulnerability Management - Perform Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/pscan/performScanStep2.jsp Go Links

Google Search 12 blocked Check AutoLink AutoFill Options

C5 Enterprise Vulnerability Management

Welcome c5evm_admin Logout **RSS** security feed

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

View Scan Definitions Create Scan Perform Scan View Scan Results

Vulnerabilities Home

Perform Vulnerability Scan

Benchmark Platforms Assets

Perform Vulnerability Scan - Step Two - Select Platform

Step 2 of 3 - Select Platform

- ☒ Microsoft Windows 2000(Assets:10)
- ☒ Microsoft Windows XP(Assets:2)
- ☒ Microsoft Windows Server 2003(Assets:3)

Back Forward

Done Internet

www.secure-elements.com

Deep asset knowledge + metadata

OVAL Scan Asset Selection

C5EVM - Vulnerability Management - Perform Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Feeds

Address http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/pscan/performScanStep2.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

View Scan Definitions

Create Scan

Perform Scan

View Scan Results

Vulnerabilities Home

Perform Vulnerability Scan - Step 3 of 3

Benchmark

Platforms

Assets

Perform

Perform Vulnerability Scan - Step Three - Select Assets

Step 3 of 3 - Select Assets

Select All

Select None

Select	Host Name	IP Address	OS Type	OS Version	Criticality	Status
<input type="checkbox"/>	W2KPRO-SP3-VM3	10.2.231.229	Microsoft Windows 2000 Professional	Service Pack 3 (Build 2195)	Medium	Protected
<input type="checkbox"/>	W2KPRO-SP1-VM2	10.2.233.235	Microsoft Windows 2000 Professional	Service Pack 1 (Build 2195)	Medium	Protected
<input checked="" type="checkbox"/>	W2KPRO-SP4-VM3	10.2.242.214	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	Medium	Protected
<input checked="" type="checkbox"/>	W2KPRO-SP0-VM2	10.2.245.238	Microsoft Windows 2000 Professional	(Build 2195)	Medium	Protected
<input type="checkbox"/>	W2KSRV-SP3-VM2	10.2.241.246	Microsoft Windows 2000 Server	Service Pack 3 (Build 2195)	Medium	Protected
<input checked="" type="checkbox"/>	W2KPRO-SP3-VM2	10.2.234.233	Microsoft Windows 2000 Professional	Service Pack 3 (Build 2195)	Medium	Protected

Done

Internet

Perform OVAL Scan

C5EVM - Vulnerability Management - Perform Vulnerability Scan - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address http://10.0.10.10:8080/c5Reports/faces/jsp/vulns/pscan/performScanStep3.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

View Scan Definitions

Create Scan

Perform Scan

View Scan Results

Vulnerabilities Home

Vulnerability scan in progress...

Benchmark

Platforms

Assets

Perform

Perform Vulnerability Scan - Step Four - Perform Scan

Scan in Progress



Go to Vulnerabilities Home

© 2005 Secure Elements All Rights Reserved.

support | about us | contact us

Done

Internet



Welcome c5evm_admin

Logout

[RSS security feed](#)

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

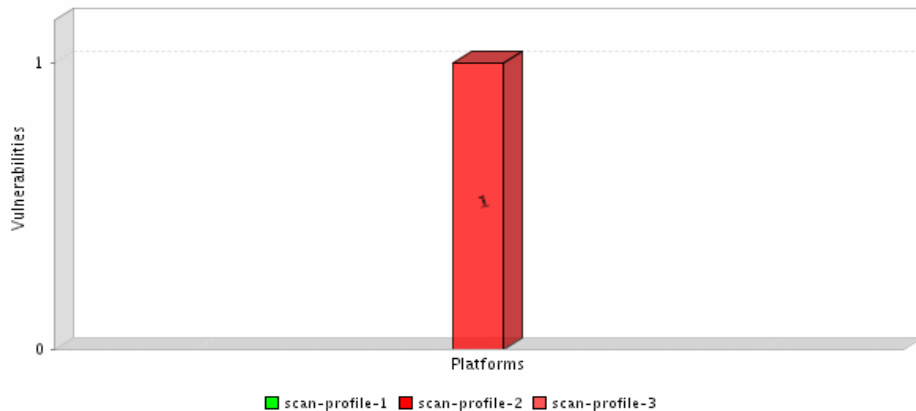
View Scan Definitions Create Scan Perform Scan View Scan Results

Vulnerabilities Home → View Scan Results

Scan Summary

Property	Value
Name	vulnerability-scan-1156201858873.xml
Source	vulnerability-scan-1156201858873.xml
Applied By	c5evm_admin
Start Time	Mon, 21 Aug 2006 11:23:13 PM GMT
Status	In Progress
# of Assets	12
# of Vulnerabilities	1

Vulnerabilities By Platform



Compliance Assessment Evaluation - Benchmark Task Details

Platform	Start time	Completion Status	# of Assets	# of Vulnerabilities
scan-profile-1	Mon, 21 Aug 2006 11:23:25 PM GMT	0 %	7	0
scan-profile-2	Mon, 21 Aug 2006 11:23:21 PM GMT	100 %	3	1
scan-profile-3	Mon, 21 Aug 2006 11:23:13 PM GMT	0 %	2	0



3 Records found, displaying 3 records, from 1 to 3. Page 1 / 1

Vulnerability Detail

C5EVM - Vulnerability Detail - Microsoft Internet Explorer provided by Secure Elements, Inc.

Drill down on those assets that have this vulnerability

Remediation for this Vulnerability

Vulnerable Assets

Remediations(5)

Vulnerability Detail

ID	oval:org.mitre.oval:def:1509	CVE ID	CVE-2006-0028
Scanner	OVAL	Severity	Medium
Name			
Excel 2003 Remote Code Execution via Malformed File Format			
Brief description			
Unspecified vulnerability in Microsoft Excel 2000, 2002, and 2003, in Microsoft Office 2000 SP3 and other packages, allows user-complicit attackers to execute arbitrary code via a BIFF parsing format file containing malformed BOOLEAN records that lead to			
Detail description			
Unspecified vulnerability in Microsoft Excel 2000, 2002, and 2003, in Microsoft Office 2000 SP3 and other packages, allows user-complicit attackers to execute arbitrary code via a BIFF parsing format file containing malformed BOOLEAN records that lead to memory corruption, probably involving invalid pointers.			
Observation			
null			
Recommendation			
null			

NVD



Enterprise Vulnerability View



Enterprise
Vulnerability
Management

Welcome c5evm_admin

Logout

security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

View Scan Definitions

Create Scan

Perform Scan

View Scan Results

Vulnerabilities

Vendor Id

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

oval:org.mit

0 1,000 2,000 3,000 4,000 5,000

Vendor

Vendor

Count

MITRE Corporation	11718
Nessus	10680
Foundstone	5195
Harris Corporation	4314
Internet Security Systems	3595
Microsoft Corporation	1278
Red Hat	1127
Security Focus	668
eEye Digital Security	602
DOD-CERT	368
Army IAVA	368
US-CERT	260
Navy IAVA	255
Air Force IAVA	83
IBM	69
Fedora Legacy	6
Secunia	4

MITRE Corporation Nessus Foundstone Harris Corporation Internet Security Systems Microsoft Corporation Red Hat
 Security Focus eEye Digital Security DOD-CERT Army IAVA US-CERT Navy IAVA Air Force IAVA IBM Fedora Legacy
 Secunia

Navy IAVA
Air Force IAVA
IBM
Fedora Legacy
Secunia

Print to Pdf

es

10

Print to Pdf

Count

0

0

0

0

872

753

11718

10680

5195

4314

3595

1278

1127

668

602

368

368

260

255

83

69

6

4

Performing the Audit

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Mail RSS 12 blocked Check AutoLink AutoFill Options

Address https://10.0.10.179/CommandCenter/faces/AssetBasedOps.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

security feed

Home Compliance Reports **Assets Management** Vulnerability Management Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Asset based Compliance Assessment - Step 1 of 4

Step 1 of 4 - Select Assets

Select All

Select None

Select OS

- ☐ All (22)
- ☐ FreeBSD (1)
- ☐ Linux (2)
- ☐ Mac OS (1)
- ☐ Solaris (3)
- ☐ Windows (15)
 - ☐ Microsoft Windows 2000 Advanced Server (2)
 - ☐ Microsoft Windows 2000 Professional (5)
 - ☐ Microsoft Windows 2000 Server (2)
 - ☐ Microsoft Windows Server 2003 Family, Standard Edition (3)
 - ☒ Microsoft Windows XP Professional(3)

Host Name	IP Address	OS Version	Criticality	Status
DBTEST1	192.168.130.196	SUSE LINUX Std Server	High	Protected
DevTEST1	192.168.130.197	SUSE LINUX Std Server	High	Disconnected
Mac-host	192.168.131.140	Mac OS X version 10.1.5	Highest	Protected
Solaris-host1	192.168.131.35	SunOS 5.9 Generic May 2002	Highest	Disconnected
Solaris-host2	192.168.131.36	SunOS 5.9 Generic May 2002	Highest	Registered
Solaris-host3	192.168.131.37	SunOS 5.9 Generic May 2002	Medium	Protected
WXPPRO-SP0-VM3	10.2.250.198	(Build 2600)	Highest	Registered
WXPPRO-SP2-VM3	10.2.251.196	Service Pack 2 (Build 2600)	Medium	Protected
WXPPRO-SP1-VM3	10.2.249.200	Service Pack 1 (Build 2600)	Highest	Registered

Forward



Dynamic Derivation of Applicable Benchmarks

C5 EVM CommandCenter - Assets summary by Operating System - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back

Address http



Home

A

By leveraging indexing information and our deep asset knowledge we are able to **derive** those benchmarks that are **relevant** for the assets selected

Logout

RSS security feed

Vulnerability Management

Remediation Management

Asset Audit

Evaluate Results

Asset - Step 2 of 4

Select Benchmark

- ☐ Windows 2000 Professional Operating System Benchmarks (cis-gold-win2000-pro-xccdf.xml)
- ☐ Windows 2000 Server Operating System Benchmarks (cis-gold-win2000-srv-xccdf.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks (cis-win2000-pro-xccdf-1.xml)
- ☐ Windows 2000 Professional Operating System Benchmarks (cis-win2000-pro-xccdf.xml)
- ☐ Windows 2000 Server Operating System Benchmarks (cis-win2000-srv-xccdf.xml)
- ☐ Windows 2000 Operating System Level One Benchmark (cis-win2000-xccdf.xml)
- ☒ SP 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professional (NIST-800-68-53-WinXPPro_XCCDF_08242006.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows 2000 (se-win2k-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark - Windows Server 2003 (se-win2k3-Best-Practices-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark (se-winxp-xccdf.xml)
- ☐ Secure Elements Best Practices Benchmark (services-xccdf.xml)

Back

Forward





Non-Technical Controls

C5 EVM CommandCenter - Compliance Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address <https://10.0.10.179/CommandCenter/faces/AssetBasedOps.jsp> Go Links



Welcome c5evm_admin

Logout

security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Asset based Compliance Assessment - Step 3 of 4

Step 3 of 4 - Answer questions

Please answer the following questions for Master Windows XP profile

1.1.1 Has your organization performed a risk analysis and assessment(s) to identify vulnerabilities and threats?

☒ TRUE ☐ FALSE ☐ UNKNOWN

1.1.2 Has your organization created an information security policy?

☒ TRUE ☐ FALSE ☐ UNKNOWN

1.1.3 Has your management team delegated a person or team to be responsible for creating and implementing the organization's information security policy (procedures, standards, guidelines, and baselines)?

☒ TRUE ☐ FALSE ☐ UNKNOWN

1.1.4 Has your organization implemented an information classification model for data?
(Business classifications: Confidential, Private, Sensitive, and Public; or Military classification: Top Secret, Secret, Confidential, Unclassified).

☒ TRUE ☐ FALSE ☐ UNKNOWN

1.1.5 Does your IT organization practice separation of duties?

☒ TRUE ☐ FALSE ☐ UNKNOWN

1.1.6 Does your organization implement a Security Awareness training program?

☒ TRUE ☐ FALSE ☐ UNKNOWN

Back

Forward



c5evm_admin

Logout

RSS security feed

Home

Compliance

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Compliance Home

Compliance Assessment Evaluation by Benchmark

Benchmark	Applied By	Start time	Completion Status	% of assets	Score
Secure Elements Best Practices Benchmark	c5evm_admin	Thu, 7 Sep 2006 08:35:02 PM GMT	In Progress	0 %	0.0 %
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Thu, 7 Sep 2006 08:32:23 PM GMT	In Progress	0 %	
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Thu, 7 Sep 2006 08:32:08 PM GMT	Not Started	0 %	
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Thu, 7 Sep 2006 08:31:38 PM GMT	Not Started	0 %	
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Thu, 7 Sep 2006 03:55:38 PM GMT	Expired	0 %	0.0 %
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Thu, 7 Sep 2006 03:55:30 PM GMT	Expired	0 %	0.0 %
Secure Elements Best Practices Benchmark	c5evm_admin	Wed, 6 Sep 2006 08:28:41 PM GMT	Completed	100 %	63.2107009887695 %
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Wed, 6 Sep 2006 08:26:09 PM GMT	Completed	50 %	22.2 %
SP 800-68: Guidance for Securing Microsoft Windows XP Systems for IT Professional	c5evm_admin	Wed, 6 Sep 2006 07:57:50 PM GMT	Completed	10 %	0.0 %
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Wed, 6 Sep 2006 07:55:33 PM GMT	Completed	100 %	32 %

Out of Compliance In Compliance



records found, displaying 10 records, from 1 to 10. Page 1 / 1

Who applied them

What is happening with them at this moment

All Benchmarks that have been run, are scheduled to run, or are running now

What was the score for all those that have completed or what is the score now for the ones in progress



Compliance Benchmark Summary

C5 EVM CommandCenter - Compliance Assessment Results - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites 12 blocked Check AutoLink AutoFill Options

Address https://10.2.2.11/CommandCenter/faces/jsp/comp/eval/benchmarkTaskSummary.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

[RSS security feed](#)

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

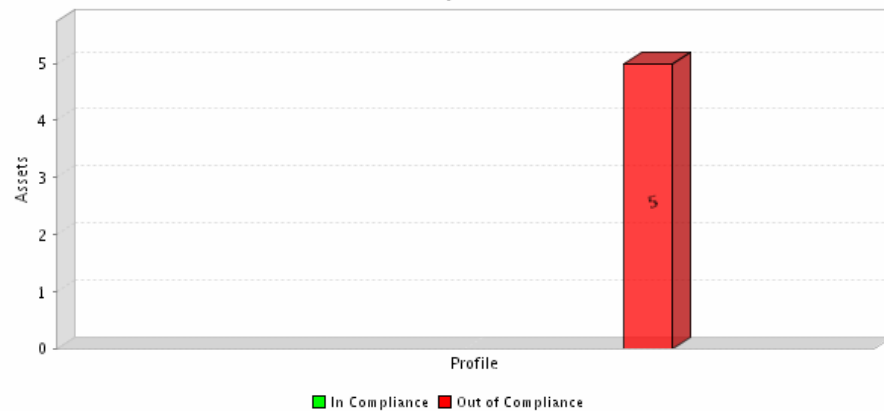
Evaluate Results

Compliance Home → Evaluate Home

Benchmark Summary

Property	Value
Name	Windows 2000 Professional Operating System Benchmarks
Source	dis-gold-win2000-pro-xccdf.xml
Applied By	c5evm_admin
Start Time	Tue, 12 Sep 2006 11:18:43 PM GMT
Status	Completed
# of Assets	5
Out of Compliance	<div><div></div></div> 100 % assets
In Compliance	<div><div></div></div> 0 % assets
Score	<div><div></div></div> 58.3333320617676 %

Score By Profile



Compliance Assessment Evaluation - Benchmark Task Details

Profile	Start time	Completion Status	Total Assets	Result	Score
Level II	Tue, 12 Sep 2006 11:18:43 PM GMT	100 %	5	<div><div></div></div> 100 % <div><div></div></div> 0 %	<div><div></div></div> 58.3333320617676 %

■ Out of Compliance ■ In Compliance

1 Records found, displaying 1 records, from 1 to 1. Page 1 / 1

Compliance Profile Summary

C5 EVM CommandCenter - Compliance Assessment Results - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Home

Address https://10.2.2.11/CommandCenter/Face



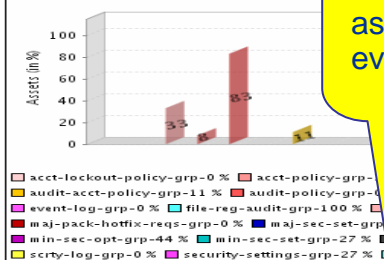
Home Compliance Assets Management Vulnerability Management

Adapt Regulatory State

Compliance Home Evaluate Home Windows Professional Operating System Benchmarks

Profile Summary	
Property	Value
Name	Level II
Benchmark	Windows 2000 Professional Op
Applied By	c5evm_admin
Start Time	Tue, 12 Sep 2006 11:18:43 P
Completion Status	100 %
# of Assets	5
Out of Compliance	100 % as
In Compliance	0 % assets
Score	58.3333320617 %

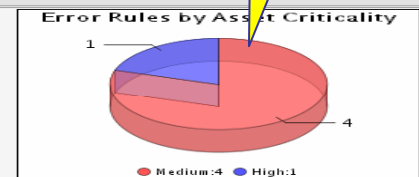
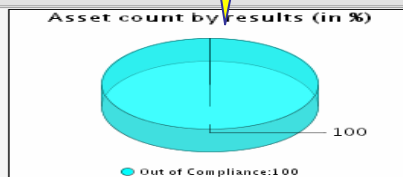
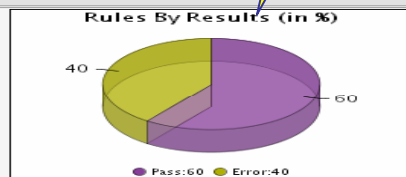
Percentage of rules that passed and failed



Percentage of assets under evaluation

Of those assets that are out of-compliance what is the distribution of their asset criticality

Is there a rule that is causing more failures than others?



Top 20 Out of Compliance Assets

Host Name	IP Address	Criticality	# failing rules	Score
W2KPRO-SP1-VM2	10.2.233.235	Medium	80	58.3333320617676
W2KPRO-SP3-VM2	10.2.234.233	Medium	80	58.3333320617676
W2KPRO-SP2-VM2	10.2.254.213	Medium	80	58.3333320617676
W2KPRO-SP4-VM2	10.2.251.221	Medium	78	59.3137283325195
SOJA-ORACLE	10.0.10.171	High	62	67.1568603515625

What assets are in the most trouble

Top 20 Failing Rules (by # of assets)

Rule Id	Title	Oval Id	# of Assets
num-prev-logon-cache-rul	Number of Previous Logons to Cache: 0	OVAL990032119	5
netmeet-remote-share-rul	NetMeeting Remote Desktop Sharing Disabled	OVAL9900419	5
sys-max-event-log-size-rul	Maximum Event Log Size	OVAL990022431	5
audit-obj-access-rul	Audit Object Access	OVAL99002215	5
int-conn-sharing-rul	Internet Connection Sharing Disabled	OVAL9900417	5
messenger-rul	Messenger Disabled	OVAL9900418	5
disable-autoplay-user-rul	Disable autoplay for the current user:	OVAL99003224	5
audit-sys-evnt-rul	Audit System Events: Success and Failure	OVAL99002219	5
allow-system-shut-wo-logon-rul	Allow System to be Shut Down Without Having to Log On: Disabled	OVAL99003212	5
ensure-icmp-routing-rul	Ensure ICMP Routing via shortest path first:	OVAL990032216	5
remote-reg-srvc-rul	Remote Registry Service Disabled	OVAL99004110	5
sys-log-retention-meth-rul	Log Retention Method	OVAL990022433	5
clear-virt-mem-shutdown-rul	Clear Virtual Memory Pagefile When System Shuts Down: Enabled	OVAL99003219	5
disable-dialin-rul	Disable Dial-in access to the server:	OVAL99003229	5
suppress-watson-rul	Suppress Dr. Watson Crash Dumps:	OVAL99003221	5
ensure-router-disc-rul	Ensure Router Discovery is Disabled:	OVAL990032220	5
sec-log-retention-meth-rul	Log Retention Method	OVAL990022423	5
rename-guest-acct-rul	Rename Guest Account: Any value other than "Guest"	OVAL990032126	5
sec-restrict-guest-rul	Restrict Guest Access	OVAL990022422	5
disable-cd-autorun-rul	Disable CD Autorun:	OVAL990032211	5



Compliance

C5EVM - ASSET COMPLIANCE DETAIL - MOZILLA FIREFOX

FILE EDIT VIEW GO BOOKMARKS TOOLS HELP

HTTP://192.168.15.10:8080/C5REPORTS/FACES/JSP/COMP/EVAL/SCANTASKDET

C5 Enterprise Vulnerability Management

Welcome c5evm admin

Home Compliance Vulnerability Management Remediation Management

Evaluate Comply

Compliance Home Evaluate Home Security Profile (aka MS Windows 2000)

Summary

HostName	W2KSSP4-C5DEMO	Status	Discovered
IP Address	192.168.15.135	Criticality	High
Sensor Version	3.0.0beta:17:42:54:May 19 2008	Confidence	High
Standard Survey Interval	-1	Remediation Strategy	Intervention
Detail Survey Interval	-1	Boot Time	0001-01-01 00:00:00.0

Asset History **Vulnerability History** **Remediation History**

Operating System & BIOS

OS Type	OS Version	BIOS Vendor
Microsoft Windows 2000 Server	Service Pack 4 (Build 2195)	PhoenixBIOS 4.0 Release 6.0

Compliance Assessment

Secure Elements Best Practices Benchmark - C5 Best Practices Profile

Score	Total Rules	Failing Rules
52.2388038635254	208	123

Failing Rules

Rule Id	Title	
profile-single-rul	Profile single process: Administrators	
system-drive-progfiles-rk-rul	%SystemDrive%\Program Files\Resource Kit	
sys-root-rsh-exe-rul	%SystemRoot%\system32\rsh.exe	OVAL990044136
mod-firmware-rul	Modify firmware environment values: Administrators	OVAL99004226
system-drive-ntdetectcom-rul	%SystemDrive%\ntdetect.com	OVAL99004418
hkml-system-ccs-hardware-profiles-rul	HKLM\System\CurrentControlSet\Hardware Profiles	OVAL990044217
sys-root-sp-uninst-rul	%SystemRoot%\\$NtServicePackUninstall\$	OVAL990044121
system-drive-msdos.sys-rul	%SystemDrive%\msdos.sys	OVAL99004416
hkml-system-cs001-rul	HKLM\System\ControlSet001	OVAL990044212
hkml-system-ccs-ctrl-sps-winreg-rul	HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg	OVAL9900442140002
sys-root-regedit-exe-rul	%SystemRoot%\regedit.exe	OVAL990044133
hkml-software-msft-windows-installer-rul	HKLM\Software\Microsoft\Windows\CurrentVersion\Installer	OVAL99004428
sys-root-reinstallbackups-rul	%SystemRoot%\system32\reinstallbackups	OVAL990044145
increase-quotas-rul	Increase quotas: Administrators	OVAL99004218
system-drive-iosys-rul	%SystemDrive%\io.sys	OVAL99004415
allow-eject-remov-ntfs-rul	Allowed to Eject Removable NTFS Media: Administrators	OVAL99003213
sys-root-debug-usermode-rul	%SystemRoot%\Debug\UserMode	OVAL990044124
hkml-system-ccs-ctrl-wmi-security-rul	HKLM\System\CurrentControlSet\Control\WMI\Security	OVAL990044215
hkml-software-msft-windows-group-policy-rul	HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy	OVAL99004427

What changed?

Any Vulnerabilities discovered lately?

Any remediations applied, bypassed?

This asset was evaluated against 208 rules of which 123 failed

Compliance Report Generation

C5 EVM CommandCenter - Reports Home - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites

Address <https://10.0.10.179/CommandCenter/faces/jsp/repo/repo28.jsp>

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

[RSS](#) [security feed](#)

[Home](#)

[Compliance](#)

[Reports](#)

[Assets Management](#)

[Vulnerability Management](#)

[Remediation Management](#)

Available Reports

Executive Reports

[Asset Remediation Executive Report](#)
[Detected Vulnerabilities Detailed Report](#)
[Enforced Policies Detailed Report](#)
[Number of Controlled Assets with Policy Violations Executive Report](#)
[Number of Controlled Assets with Vulnerabilities Executive Report](#)
[Number of Violations Executive Report](#)
[Percent of Controlled Assets with Policy Violations Executive Report](#)
[Percent of Controlled Assets with Vulnerabilities Executive Report](#)
[Percentage of Violations Executive Report](#)
[Violated Policies Detailed Report](#)
[Vulnerability and Policy Compliance Assessment](#)

Standard Reports

[Software Inventory](#)
[Alert View](#)
[Applied Policy View](#)
[Asset Detail View](#)
[Asset Log View](#)
[Retired Asset View](#)
[Asset Uptime View](#)
[Audit Log View](#)
[C5EVM Users View](#)
[Installed Application View](#)
[Installed Patch View](#)
[Killed Process View](#)
[Running Process View](#)
[Ungrouped Asset View](#)
[Violated Policy View](#)
[Vulnerability View](#)
[Asset Compliance](#)

Report Criteria

Asset Compliance

The Asset Compliance report provides compliance score for an asset.

Specify the asset selection criteria

- ☒ By IP Address
☐ By Host Name
☐ By Group

[Run Report](#)

Enterprise
Vulnerability
Management

Welcome c5evm_admin

Logout

[RSS security feed](#)[Home](#)[Compliance](#)[Reports](#)[Assets Management](#)[Vulnerability Management](#)[Remediation Management](#)

Summary

HostName	W2KPRO-SP4-VM2	Status	Disconnected
IP Address	10.2.251.221	Criticality	High
Sensor Version	3.0.0beta:12:11:55:Aug 16 2006	Confidence	High
OS Type	Microsoft Windows 2000 Professional	Remediation Strategy	Intervention
OS Version	Service Pack 4 (Build 2195)		

Benchmarks Summary

Benchmark	Applied By	Start time	Completion Status	Score
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Thu, 7 Sep 2006 03:55:38 PM EDT	In Progress	0.0 %
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Thu, 7 Sep 2006 03:55:30 PM EDT	In Progress	0.0 %
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Wed, 6 Sep 2006 07:55:33 PM EDT	Completed	<div></div> 39.5348854064941 %



Detailed Asset Compliance Report

Asset Compliance - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Home

Address <https://10.0.10.179/CommandCenter/faces/jsp/repo/assetComplianceSummaryReport.jspx>

Google Search 12 blocked Check AutoLink AutoFill Options



Enterprise
Vulnerability
Management

Welcome c5evm_admin

Logout

[RSS](#) [Security feed](#)

Home Compliance Reports Assets Management Vulnerability Management Remediation Management

Summary

HostName	W2KPRO-SP4-VM2	Status	Disconnected
IP Address	10.2.251.221	Criticality	High
Sensor Version	3.0.0beta:12:11:55:Aug 16 2006	Confidence	High
OS Type	Microsoft Windows 2000 Professional	Remediation Strategy	Intervention
OS Version	Service Pack 4 (Build 2195)		

Compliance Assessment against the Secure Elements Best Practices Benchmark - Windows 2000

Score	Total Rules	Failing Rules
39.5348854064941	251	156

Failing Rules

Rule Id	Title	Oval Id
audit-dir-srvc-access-rul	Audit Directory Service Access: Not Defined	OVAL99002213
max-pw-age-rul	Maximum Password Age	OVAL9900212
tcp-allowed-ports-rul	TCP Allowed Ports are Enabled: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPAllowedPorts (REG_DWORD) 1	oval:com.secure-elements:def:9201703076
sec-log-retention-rul	Log Retention	OVAL990022424
protect-dflt-gateway-rul	Protect the Default Gateway network setting: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect (REG_DWORD) 0	OVAL990032215
windows-installer-rul	Windows Installer - Disabled	oval:com.secure-elements:def:9201703067
alerter-rul	Alerter - Disabled	OVAL9900411
app-log-retention-rul	Log Retention	OVAL990022414
kerberos-key-dist-rul	Kerberos Key Distribution Center - Disabled	oval:com.secure-elements:def:9201703023
iis-admin-srvc-rul	IIS Admin Service - Disabled	OVAL9900416
disable-auto-debug-rul	Disable Automatic Execution of the System Debugger: HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto (REG_DWORD) 0	OVAL99003222
computer-browser-rul	Computer Browser - Disabled	OVAL9900413
qos-rsvp-wkstn-rul	QoS RSVP - Disabled	oval:com.secure-elements:def:9201703040
msdtc-rul	Distributed Transaction Coordinator - Disabled	oval:com.secure-elements:def:9201703013
qos-rsvp-svr-rul	QoS Admission Control (RSVP) - Disabled	oval:com.secure-elements:def:9201703039
syn-attck-protect-retried-rul	SYN Attack protection - Manage TCP Maximum half-open retried sockets: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenretried (REG_DWORD) 80 or 400	OVAL990032223
dhcp-client-rul	DHCP Client - Disabled	oval:com.secure-elements:def:9201703008
messenger-rul	Messenger - Disabled	OVAL9900418
rename-guest-acct-rul	Rename Guest Account: Any value other than 'Guest'	OVAL990032126
distrib-link-client-rul	Distributed Link Tracking Client - Disabled	oval:com.secure-elements:def:9201703011
wmi-driver-rul	Windows Management Instrumentation Driver Extensions - Disabled	oval:com.secure-elements:def:9201703070
hklm-system-currentcontrolset-control-contentindex-rul	HKLM\System\CurrentControlSet\Control\ContentIndex	oval:com.secure-elements:def:9201703083
removable-storage-rul	Removable Storage - Disabled	oval:com.secure-elements:def:9201703049
protected-storage-rul	Protected Storage - Disabled	oval:com.secure-elements:def:9201703038
sys-restrict-guest-rul	Restrict Guest Access	OVAL990022432
hklm-system-currentcontrolset-services-tcpip-rul	HKLM\System\CurrentControlSet\Services\Tcpip	oval:com.secure-elements:def:9201703089
utility-manager-rul	Utility Manager - Disabled	oval:com.secure-elements:def:9201703066
manage-keep-alive-rul	Manage Keep-alive times: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime (REG_DWORD) 300000	OVAL990032218
telnet-rul	Telnet - Disabled	OVAL99004115

Enterprise Compliance

C5 EVM CommandCenter - Compliance Assessment Results - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address https://10.2.2.11/CommandCenter/faces/jsp/comp/eval/benchmarkTaskSummary.jsp

Google Search 12 blocked Check AutoLink AutoFill Options



Welcome c5evm_admin

Logout

RSS security feed

Home

Compliance

Reports

Assets Management

Vulnerability Management

Remediation Management

Adapt Regulatory Standard

Perform Compliance Audit

Evaluate Results

Compliance Home

Compliance Assessment Evaluation by Benchmark

Benchmark	Applied By	Start time	Completion Status	% of assets	Score
Secure Elements Best Practices Benchmark	c5evm_admin	Thu, 7 Sep 2006 08:35:02 PM GMT	In Progress	0 % <div></div> 100 %	0.0 %
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Thu, 7 Sep 2006 08:32:23 PM GMT	In Progress	0 % <div></div> 100 %	0.0 %
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Thu, 7 Sep 2006 08:32:08 PM GMT	Not Started	0 % <div></div> 100 %	0.0 %
Secure Elements Best Practices Benchmark - Windows Server 2003	c5evm_admin	Thu, 7 Sep 2006 08:31:38 PM GMT	Not Started	0 % <div></div> 100 %	0.0 %
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Thu, 7 Sep 2006 03:55:38 PM GMT	Expired	0 % <div></div> 100 %	0.0 %
Secure Elements Best Practices Benchmark - Windows 2000	c5evm_admin	Thu, 7 Sep 2006 03:55:38 PM GMT	Expired	0 % <div></div> 100 %	0.0 %

- Leveraged Many Man Years of SME from SE, CIS, DISA, NSA/NIST, etc.
- Enabled enterprise wide evaluation of assets on demand
- Identified those assets that are out of compliance/vulnerable and why
- Memorialized what has been done in the database
- Report on it at will



- Pareto's principle
 - "for many phenomena 80% of consequences stem from 20% of the causes."
- 80% Use cases can be addressed by the abstraction
- 20% Require getting out of the abstraction

C5 Helium Content "Browser"

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites AutoFill Options

Address https://10.2.2.11/CommandCenter/faces/jsp/home.jsp

Google

C5 Enterprise Vulnerability Manager

Home

Login To Server



Helium

☒ Specify EM Host Name ☐ Specify Host URL

Host:

LOGIN

CANCEL

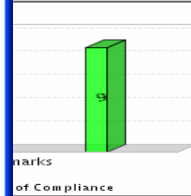
Logout

RSS Security feed

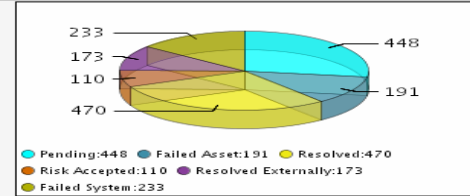
Vulnerability Management

Remediation Management

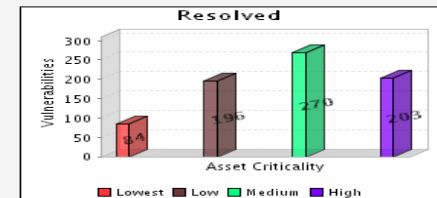
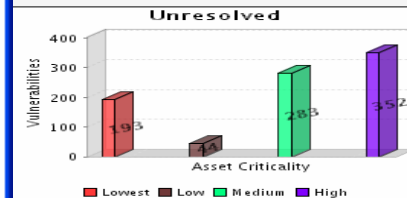
Compliance Benchmarks



Vulnerabilities By Status



Vulnerabilities By Asset Criticality



Top 10 Most Vulnerable Assets

Export to Pdf

Host	IP Address	# of Vulns	OS type	OS version	Criticality	Status
SOJA-ORACLE	10.0.10.171	165	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Protected
W2K3SSPO02K31-3	10.2.243.248	138	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Lowest	Protected
W2K3SSPO02K31-2	10.2.232.235	132	Microsoft Windows Server 2003 Family, Standard Edition	(Build 3790)	Medium	Protected
W2KPRO-SP4-VM2	10.2.251.221	118	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	High	Disconnected
W2KASRV-SP4-VM2	10.2.251.230	77	Microsoft Windows 2000 Advanced Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KSRV-SP4-VM2	10.2.248.237	50	Microsoft Windows 2000 Server	Service Pack 4 (Build 2195)	Medium	Protected
W2KPRO-SP3-VM3	10.2.231.229	49	Microsoft Windows 2000 Professional	Service Pack 3 (Build 2195)	Lowest	Protected
W2KPRO-SP2-VM2	10.2.254.213	46	Microsoft Windows 2000 Professional	Service Pack 2 (Build 2195)	High	Protected
W2KPRO-SP4-VM3	10.2.242.214	30	Microsoft Windows 2000 Professional	Service Pack 4 (Build 2195)	Low	Protected
W2KSRV-SP3-VM2	10.2.241.246	24	Microsoft Windows 2000 Server	Service Pack 3 (Build 2195)	Medium	Protected

Top 10 Unresolved Vulnerabilities (by # of occurrences)

Export to Pdf

Vendor Id	Name	CVE/CAN Id	Severity	# of Occurrences
oval.org.mitre.oval:def:115	Hyperlink Object Function Vulnerability	CVE-2006-3438	High	10
oval.org.mitre.oval:def:13	Buffer Overrun in HTML Help Vulnerability	CVE-2006-3357	High	8
oval.org.mitre.oval:def:155	User Profile Elevation of Privilege Vulnerability	CVE-2006-3443	High	8
oval.org.mitre.oval:def:21	Microsoft Office Remote Code Execution Using a Malformed GIF Vulnerability	CVE-2006-0007	High	8
oval.org.mitre.oval:def:492	Buffer Overrun in Server Service Vulnerability	CVE-2006-3439	High	8
oval.org.mitre.oval:def:841	Unhandled Exception Vulnerability	CVE-2006-3648	High	8
oval.org.mitre.oval:def:1559	Windows Media Player Plug-in EMBED Vulnerability	CVE-2006-0005	Medium	8
oval.org.mitre.oval:def:723	DNS Client Buffer Overrun Vulnerability	CVE-2006-3441	High	7
oval.org.mitre.oval:def:747	Winsock Hostname Vulnerability	CVE-2006-3440	High	7
oval.org.mitre.oval:def:999	Hyperlink Object Buffer Overflow Vulnerability	CVE-2006-3086	High	7



C5 - Content Browser

File Edit Tools

http://checklists.

- XCCDF Benchmark 1.0
- XCCDF Benchmark 1.0
- XCCDF Benchmark 1.1
- OVAL 4.1
- OVAL 5.0 RC3
- CIS Interactive Survey 0.1
- SecLabs Compliance 1.0
- SecLabs Scan 1.0
- Common Alerting Protocol (CAP) 1.1

It's all about schema in general, not specific to OVAL or XCCDF

Legend: Entity, Entity Reference, Item, Attribute, List



Schema Awareness

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back C5 - Content Browser

Address Google File Edit Tools XCCDF Benchmark 1.1

http://checklists.nist.gov/xccdf/1.1/Benchmark (2)

Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml
Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

Export Benchmark

Create copy of Benchmark

Delete Benchmark

Commit changes to Benchmark

Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

Export Benchmark

Create copy of Benchmark

Delete Benchmark

Commit changes to Benchmark

- add Id
- add rear-matter
- add plain-text
- add platform-definitions
- add metadata
- add Value
- add Rule
- add TestResult
- add signature

Vulnerabilities

Host

SOJA-OR

W2K3SSP

3

W2K3SSP

2

W2KPRO

W2KASRV

VM2

W2KSRV

W2KPRO

W2KPRO

W2KPRO

W2KPRO

W2KSRV

Co

t

Legend: Entity, Entity Reference, Item, Attribute, List



Profiles

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back
C5 - Content Browser

Address
Google File Edit Tools XCCDF Benchmark 1.1

- http://checklists.nist.gov/xccdf/1.1/Benchmark (2)
 - Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml
 - resolved=false
 - id=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml
 - lang=en
 - status=accepted
 - title (1)
 - description (1)
 - notice (1)
 - front-matter (1)
 - rear-matter (0)
 - reference (2)
 - plain-text (0)
 - Platform-Specification
 - platform (1)
 - version=Professional
 - metadata (0)
 - model (2)
 - Profile (12)
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Moderate
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-High
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Low
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Moderate
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-High
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Low
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Moderate
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-High
 - Value (0)
 - Group (17)
 - Rule (0)
 - TestResult (0)
 - Benchmark=se-win2k3-Best-Practices-xccdf.xml#se-win2k3-Best-Practices-xccdf.xml

Name: Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

Context: The benchmark tag is the top level element representing a complete security checklist, including descriptive text and test items.



Simple Editing

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back C5 - Content Browser

Address File Edit Tools XCCDF Benchmark 1.1

http://checklists.nist.gov/xccdf/1.1: Benchmark (2)

- Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml
 - resolved=false
 - id=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml
 - lang=en
 - status=accepted
 - date=2005-11-05
 - title (1)
 - description (1)
 - notice (1)
 - front-matter (1)
 - rear-matter (0)
 - reference (2)
 - plain-text (0)
 - Platform-Specification
 - platform (1)
 - version=Professional
 - metadata (0)
 - model (2)
 - Profile (12)
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Moderate
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-High
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Low
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Moderate
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-High
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Low
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Moderate
 - Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-High
 - Value (0)
 - Group (17)
 - Rule (0)
 - TestResult (0)
- Benchmark=se-win2k3-Best-Practices-xccdf.xml#se-win2k3-Best-Practices-xccdf.xml

status

Enter value for status

accepted

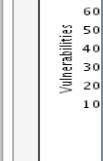
accepted deprecated draft incomplete interim

EN EL

Name: status=accepted

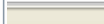
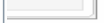
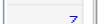
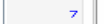
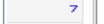
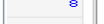
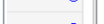
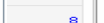
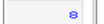
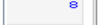
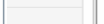
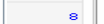
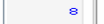
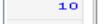
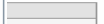
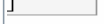
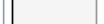
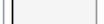
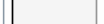
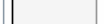
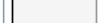
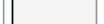
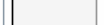
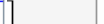
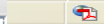
Context: The acceptance status of an Item with an optional date attribute that signifies the date of the status change.

Content: accepted



Host
SOJA-OF
W2K3SS3
W2K3SS2
W2KPRC
W2KASR VM2
W2KSRV
W2KPRC
W2KPRC
W2KPRC
W2KSRV

Go Links



C5 EVM - Com **C5 - Content Browser** **Benchmark 1.1**

File Edit Tool

Address [https://csrc.nist.gov/xccdf/1.1/Benchmark\(2\)](https://csrc.nist.gov/xccdf/1.1/Benchmark(2))

Google

C5

Home

Wind FreeB

Vulnerabilities

600
500
400
300
200
100
0

Min

Host

SOJA-ORACLE

W2K3SSP002K3

W2K3SSP002K2

W2KPRO-SP4-V

W2KASRV-SP4-VM2

W2KSRV-SP4-V

W2KPRO-SP3-V

W2KPRO-SP2-V

W2KPRO-SP4-V

W2KSRV-SP3-V

© 2005 Secure Ele

Benchmark 1.1

http://csrc.nist.gov/xccdf/1.1/Benchmark(2)

Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

resolved=1

id=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

lang=en

status=interim

title (1)

description (1)

notice (1)

front-matter (1)

rear-matter (0)

reference (2)

plain-text (0)

Platform-Specification

platform (1)

version=Professional

metadata (0)

model (2)

Profile (12)

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Moderate

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-High

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Low

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-Moderate

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Enterprise-High

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Specialized-Security-Limited

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Low

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-Moderate

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#Legacy-High

Value (0)

Group (17)

Rule (0)

TestResult (0)

Benchmark=se-win2k3-Best-Practices-xccdf.xml#se-win2k3-Best-Practices-xccdf.xml

Name: status=interim

Context: The acceptance status of an Item with an optional date attribute that signifies the date of the status change.

Content: interim

Links

PDF

10
8
8
8
8
8
7
7
7

Inter-Source Updating

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit Tools XCCDF Benchmark 1.1

Address http://checklists.nist.gov/xccdf/1.1/Benchmark (1)

Google

Back

File Edit Tools

lang=en
resolved=false
id=Windows-XP-SP-800-68-1
status=accepted
title (1)
description (1)
notice (1)
front-matter (1)
reference (2)
Platform-Specification
platform (1)
version=Professional
model (2)
Profile (...)

Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low

prohibitChanges=false
abstract=false
id=SOHO-Standalone-Low
title (1)
select (...)

select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#AccessControlChecks
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#AC-1
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordHistoryEnforcement

selected=true
idref=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordHistoryEnforcement <Rule>

selected=true
prohibitChanges=false
hidden=false
abstract=false
severity=unknown
extends=false
role=full
id=PasswordHistoryEnforcement
weight=1.0
title (1)
description (1)
check

selector
system=http://oval.mitre.org/OVAL/XML...
check-content-ref
href=WindowsXP-SP800-68.xml

name=WindowsXP-SP800-68.xml#oval:gov.nist.1:def.6 <definition>
deprecated=false
class=compliance
id=oval:gov.nist.1:def.6
version=1
metadata
criteria

select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MaximumPasswordAge
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordAge
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordLength-8
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordLength-12
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordComplexity
select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordStorageReversibleEncryption

Host

SOJA-C
W2K3S
3
W2K3S
2
W2KPR
W2KAS
VM2
W2KSR
W2KPR
W2KPR
W2KPR
W2KPR
W2KSR

Vulnerabilities

6
5
4
3
2
1

Export to Pdf

ity	# of Occurrences
	10
	8
	8
	8
	8
	8
m	8
	7
	7
	7

Legend: Entity, Entity Reference, Item, Attribute, List

Internet

- Selection reference from the profile to a rule in the same source.
- A 'check' reference from the rule to an oval definition in another source



Legend:  Entity,  Entity Reference,  Item,  Attribute,  List



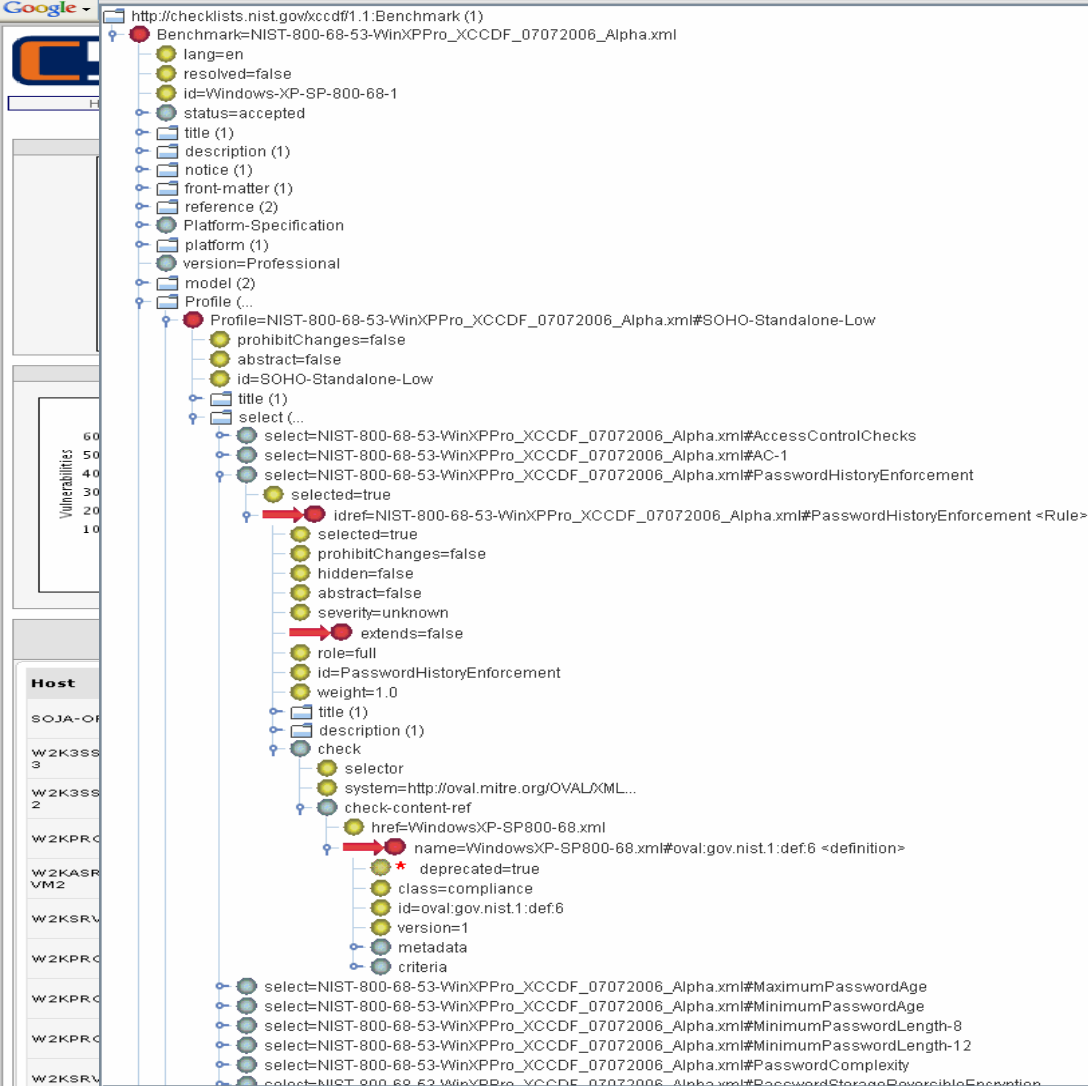
Inter-Source Updating

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit View Favorites Tools Help

Back C5 - Content Editor

Address File Edit Tools XCCDF Benchmark 1.1



Legend: Entity, Entity Reference, Item, Attribute, List

Print to Pdf

ences

10
8
8
8
8
8
7
7
7

Inter-Source Updating

C5 EV C5 - Content Editor

File Edit Tools XCCDF Benchmark 1.1

Address http://checklists.nist.gov/xccdf/1.1: Benchmark (1)

Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

- lang=en
- resolved=false
- id=Windows-XP-SP-800-68-1
- status=accepted
- title (1)
- description (1)
- notice (1)
- front-matter (1)
- reference (2)
- Platform-Specification
- platform (1)
- version=Professional
- model (2)
- Profile (...)
- Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low
 - prohibitChanges=false
 - abstract=false
 - id=SOHO-Standalone-Low
 - title (1)
 - select (...)
 - select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#AccessControlChecks
 - select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#AC-1
 - select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordHistoryEnforcement
 - selected=true
 - idref=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordHistoryEnforcement <Rule>
 - selected=true
 - prohibitChanges=false
 - hidden=false
 - abstract=false
 - severity=unknown
 - extends=false
 - role=full
 - id=PasswordHistoryEnforcement
 - weight=1.0
 - title (1)
 - description (1)
 - check
 - selector
 - system=http://oval.mitre.org/OVALXML...
 - check-content-ref
 - href=WindowsXP-SP800-68.xml
 - name=WindowsXP-SP800-68.xml#oval:gov.nist.1:def:6 <definition>
 - Save oval definitions
 - Delete definition
 - add notes

- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MaximumPasswordAge
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordAge
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordLength-8
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordLength-12
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordComplexity
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordStorageReversibleEncryption

Legend: ● Entity, → Entity Reference, ● Item, ● Attribute, □ List

to Pdf

ces

10

8

8

8

8

8

8

7

7

7

7

7

7

7

7

7

7

7

7

7



Inter-Source Updating

C5 EVM - CommandCenter - Microsoft Internet Explorer provided by Secure Elements, Inc.

File Edit Tools XCCDF Benchmark 1.1

Address http://checklists.nist.gov/xccdf/1.1/Benchmark (1)

Benchmark=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml

- lang=en
- resolved=false
- id=Windows-XP-SP-800-68-1
- status=accepted
- title (1)
- description (1)
- notice (1)
- front-matter (1)
- reference (2)
- Platform-Specification
- platform (1)
- version=Professional
- model (2)
- Profile (...)
- Profile=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#SOHO-Standalone-Low
 - prohibitChanges=false
 - abstract=false
 - id=SOHO-Standalone-Low
 - title (1)
 - select (...)
 - select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#AccessControlChecks
 - select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#AC-1
 - select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordHistoryEnforcement
 - selected=true
 - idref=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordHistoryEnforcement <Rule>
 - selected=true
 - prohibitChanges=false
 - hidden=false
 - abstract=false
 - severity=unknown
 - extends=false
 - role=full
 - id=PasswordHistoryEnforcement
 - weight=1.0
 - title (1)
 - description (1)
 - check
 - selector
 - system=http://oval.mitre.org/OVAL/XML...
 - check-content-ref
 - href=WindowsXP-SP800-68.xml
 - name=WindowsXP-SP800-68.xml
 - deprecated=true
 - class=compliance
 - id=oval.gov.nist.1:def.6
 - version=1
 - metadata
 - criteria

- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MaximumPasswordAge
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordAge
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordLength-8
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#MinimumPasswordLength-12
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordComplexity
- select=NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml#PasswordStorageReversibleException

Save oval_definitions

Save In: nist

CVS

- NIST-800-68-53-WinXPPro_XCCDF_07072006_Alpha.xml
- upload.registry
- WindowsXP-SP800-68.xml

File Name: WindowsXP-SP800-68.xml

Files of Type: *.xml or *.registry file

Save Cancel

Legend: Entity, Entity Reference, Item, Attribute, List



Audit. Evaluate. Comply.

"It really is that simple"



Questions?